

# Pseudo-Wigner Matrices from Dual BCH Codes

Ilya Soloveychik, Yu Xiang and Vahid Tarokh,  
John A. Paulson School of Engineering and Applied Sciences,  
Harvard University

**Abstract**—We consider the problem of generating pseudo-random matrices based on the similarity of their spectra to Wigner’s semicircular law. We introduce  $r$ -independent pseudo-Wigner ensembles and prove closeness of their spectra to the semicircular density in Kolmogorov distance. We give an explicit construction of a family of  $N \times N$  pseudo-Wigner ensembles using dual BCH codes and show that the Kolmogorov complexity of the obtained matrices is of the order of  $\log(N)$  for a fixed Kolmogorov distance precision. We compare our construction to the quasi-random graphs introduced by Chung, Graham and Wilson and demonstrate that the pseudo-Wigner matrices pass stronger randomness tests than the adjacency matrices of these graphs (lifted by the mapping  $0 \rightarrow 1$  and  $1 \rightarrow -1$ ) do. Finally, we provide numerical simulations verifying our theoretical results.

**Index Terms**—Pseudo-Random matrices, semicircular law, Wigner ensemble, BCH code.

## I. INTRODUCTION

Random matrices have been a very active area of research for the last few decades and have found enormous amount of applications in various areas of modern mathematics, physics, engineering, biological modeling, and other fields [1]. In this article, we focus on square symmetric matrices with  $\pm 1$  entries, referred to as square symmetric *sign* matrices. For such matrices, Wigner [2] demonstrated that if the elements of the upper triangle of an  $N \times N$  square symmetric matrix are independent Rademacher ( $\pm 1$  with equal probabilities) random variables, then as  $N$  grows, a properly scaled empirical spectral distribution converges to the semi-circle law in distribution.

In many engineering applications, one needs to simulating random matrices. The most natural way to generate an instance of a random  $N \times N$  sign matrix is to toss a fair coin  $\frac{N(N+1)}{2}$  times, fill the upper triangular part of a matrix with the outcomes

and reflect the upper triangular part into the lower. Unfortunately, for large  $N$  such approach would require a powerful source of randomness due to the independence condition [3]. In addition, when the data is generated by a truly random source, atypical *non-random looking* outcomes have non-zero probability of showing up. Yet another issue is that any experiment involving tossing a coin would be impossible to reproduce. All these reasons motivated researchers and engineers to seek for different approaches of generating *random-looking* data, especially for applications in cryptography, digital signal processing, navigation systems, scrambling, coding theory, etc. [4]. This has motivated the study of *pseudo-random* sources of binary digits [4, 5].

The word *pseudo-random* is used to emphasize that the binary data at hand is indeed generated by an entirely deterministic causal process with low algorithmic complexity, but its statistical properties resemble some of the properties of data generated by tossing a fair coin. Most efforts were focused on one dimensional pseudo-randomness [4, 5] due to their natural applications and to the relative simplicity of their analytical treatment. One of the most popular methods of generating pseudo-random sequences is due to Golomb [5] and is based on linear feedback shift registers capable of generating pseudo-random sequences of very low algorithmic complexity. The study of pseudo-random arrays and matrices was launched around the same time [6–9]. Among the known two dimensional pseudo-random constructions the most popular are the so-called perfect maps [6, 10, 11], and two dimensional cyclic codes [8, 9]. However, none of these works considered spectral properties as the defining statistical features for their constructions.

There exist various approaches to quantify the algorithmic power needed to generate an individual piece of binary data, also known as algorithmic

complexity [12–14]. It can be intuitively thought of as a measure of amount of randomness stored in that piece of data. Below we stick to the concept of Kolmogorov complexity [15, 16]. Let  $D$  be a string of binary data of length  $n$ , then its Kolmogorov complexity is the length of the shortest binary Turing machine code that can produce  $D$  and halt. If  $D$  has no computable regularity it cannot be encoded by a program shorter than its original length  $n$  (here and below the Kolmogorov complexity is given up to an additive constant), meaning that its consecutive bits are unpredictable given the preceding ones and it may be considered as truly random [13, 17]. A string with a regular pattern, on the other hand, can be computed by a program much shorter than the string itself, thus having a much smaller Kolmogorov complexity. By convention, a comparison of Kolmogorov complexities of various strings of the same length is usually done by conditioning on the length and, thus, assuming the length to be already known to the machine without specifying it as an input [18]. For example, the conditional Kolmogorov complexity of a Golomb sequence of length  $n$  is  $2\log_2 n$ , which is relatively small, since using a simple combinatorial argument one can show that at most  $\frac{n}{2^n}$  fraction of the strings of length  $n$  have conditional Kolmogorov complexity less than  $\log_2 n$ .

Specific pseudo-random sequence and array constructions usually start with a set of properties mimicking truly random data, and attempt to come up with deterministic ways of reproducing these properties. Following this approach, given a precision parameter  $\varepsilon \geq \frac{1}{\log_2 N}$ , we propose an explicit construction of scaled  $N \times N$  symmetric sign matrices with high probability possessing spectra within  $\varepsilon$ -vicinity (in Kolmogorov distance) of the semicircular law and having conditional Kolmogorov complexity proportional to  $\frac{1}{\varepsilon} \log_2 N$ .

The main contributions of this paper are as follows. First, we introduce a concept of  $r$ -independent pseudo-Wigner matrices and prove closeness of their spectra to the semicircular law. Second, we give an explicit deterministic construction of such matrices which may replace random matrices generators in engineering applications. Third, using this construction we upper bound the amount of randomness needed to obtain Wigner’s semicircular property, and show that it is surprisingly low. We also compare the proposed concept of pseudo-

Wigner matrices with incidence matrices of the quasi-random graphs suggested by Chung, Graham and Wilson [19] (lifted by the mapping  $0 \rightarrow 1$ , and  $1 \rightarrow -1$ ) and show that our construction passes wider tests for randomness.

The outline of this paper is given next. In Section II, we start with setting the notations and discussing a number of auxiliary results. We define  $r$ -independent pseudo-Wigner ensembles, and analyze their spectral properties in Section III. In Section IV we provide an explicit construction of such matrices. We analyze the Kolmogorov complexity of semicircular law in Section V. The relation of the pseudo-Wigner matrices to the quasi-random graphs is explored in Section VI. We support our theoretical investigation by numerical experiments in Section VII and provide our conclusions and final remarks in Section VIII.

## II. NOTATIONS

For a vector  $\mathbf{x} \in \mathbb{R}^N$ , let  $\|\mathbf{x}\|$  denote its Euclidean norm (length), and for a real symmetric matrix  $\mathbf{M} \in \mathbb{R}^{N \times N}$ , we denote its spectral norm by

$$\|\mathbf{M}\| = \max_{\mathbf{x} \in \mathbb{R}^N, \|\mathbf{x}\|=1} \mathbf{x}^T \mathbf{M} \mathbf{x}. \quad (1)$$

For a real  $x$ ,  $\lfloor x \rfloor$  stands for the largest integer not exceeding  $x$ , and  $\lceil x \rceil$  stands for the smallest integer not less than  $x$ .

**Random variables.** For a real random variable  $X$ , we denote by  $F_X(x)$  its cumulative distribution function (c.d.f.) and by  $f_X(x)$  the corresponding probability density function (p.d.f.). The  $p$ -th central moment of  $X$  is denoted by  $M_p(X) = \mathbb{E}[(X - \mathbb{E}X)^p]$  when it exists. The second moment will also be denoted by  $\text{var}[X] = M_2(X)$ . If a sequence of random variables  $X_N$  converges in distribution to a law  $\mathcal{F}$ , we write  $X_N \xrightarrow{D} \mathcal{F}$ .

We denote by  $S_N$  the set of all symmetric  $N \times N$  matrices with entries  $\pm \frac{1}{2\sqrt{N}}$ . The Wigner ensemble  $\mathcal{W}_N$  is defined as the set  $S_N$  endowed with the uniform probability measure.

**Binary linear codes.** Let  $\mathcal{C}$  be an  $[n, k, d]$  binary linear code of length  $n$ , dimension  $k$  and minimum Hamming distance  $d$  over the field  $GF(2)$ . We say that two words  $\mathbf{u} = \{u_i\}$ ,  $\mathbf{v} = \{v_i\} \in GF(2)^n$  are orthogonal if  $\sum_i v_i u_i = 0$  in  $GF(2)$ . The dual code  $\mathcal{C}^\perp$  of  $\mathcal{C}$  is a linear code of length  $n$  and dimension  $k^\perp = n - k$ , whose codewords are orthogonal to all the codewords of  $\mathcal{C}$ .

Let also

$$\begin{aligned} \zeta : GF(2)^N &\rightarrow \{-1, 1\}^N, \\ (u_1, \dots, u_N) &\mapsto ((-1)^{u_1}, \dots, (-1)^{u_N}). \end{aligned} \quad (2)$$

### III. PSEUDO-WIGNER ENSEMBLES

For any symmetric matrix  $\mathbf{A}_N \in S_N$ , denote by  $F_{\mathbf{A}_N}$  the c.d.f. associated with its spectrum  $\{\lambda_i\}_{i=1}^N$ ,

$$F_{\mathbf{A}_N}(x) = \frac{1}{N} \sum_{i=1}^n \theta(x - \lambda_i), \quad (3)$$

where  $\theta(x)$  is the unit step function at zero. The  $l$ -th moment of  $\mathbf{A}_N$  is given by

$$\beta_l(\mathbf{A}_N) = \int x^l dF_{\mathbf{A}_N} = \frac{1}{N} \text{Tr}(\mathbf{A}_N^l). \quad (4)$$

Let  $F_{sc}$  be the c.d.f. of the standard semicircular law

$$F_{sc}(x) = \frac{1}{2} + \frac{1}{\pi} x \sqrt{1 - x^2} + \frac{1}{\pi} \arcsin(x), \quad -1 \leq x \leq 1, \quad (5)$$

with the corresponding p.d.f.

$$f_{sc}(x) = \frac{2}{\pi} \sqrt{1 - x^2}, \quad -1 \leq x \leq 1. \quad (6)$$

The moments of this distribution read as

$$\beta_l = \int_{-\infty}^{\infty} x^l dF_{sc} = \begin{cases} 0, & l \text{ odd}, \\ \frac{1}{2^l} \frac{l!}{(\frac{l}{2})! (\frac{l}{2}+1)!}, & l \text{ even}. \end{cases} \quad (7)$$

#### A. The Semicircular Law and the Wigner Ensemble

Recall that the Wigner ensemble  $\mathcal{W}_N$  was defined to be the set  $S_N$  endowed with the uniform probability measure.

**Lemma 1** (Main Theorem from [20]). *Let  $\mathbf{W}_N \in \mathcal{W}_N$ , then as  $N$  tends to infinity,*

$$\mathbb{E}[\beta_l(\mathbf{W}_N)] = \begin{cases} 0, & l \text{ odd}, \\ \beta_l + o(1), & l \text{ even}, \end{cases} \quad (8)$$

and the random variable  $N(\beta_l(\mathbf{W}_N) - \mathbb{E}[\beta_l(\mathbf{W}_N)])$  converges in distribution to the normal law

$$N(\beta_l(\mathbf{W}_N) - \mathbb{E}[\beta_l(\mathbf{W}_N)]) \xrightarrow{D} \mathcal{N}\left(0, \frac{1}{\pi}\right), \quad (9)$$

in particular,

$$M_p(N\beta_l(\mathbf{W}_N)) = \begin{cases} 0, & p \text{ odd}, \\ \frac{(p-1)!!}{\pi^{p/2}} + o(1), & p \text{ even}. \end{cases} \quad (10)$$

This result in particular implies almost sure weak convergence of the empirical spectra of matrices from the Wigner ensemble to the semicircular law.

#### B. Pseudo-Wigner Ensemble

Let us now introduce an ensemble of matrices matching the behavior of Wigner matrices up to a certain moment. Later we will show that if the number of matching moments grows logarithmically with the matrix size  $N$ , the empirical spectrum converges to the semicircular law with high probability.

**Definition 1** (*r*-independence of a sequence). *Let  $\mathbf{x} = \{X_i\}_{i=1}^N$  be a sequence of binary random variables. We say that  $\mathbf{x}$  is *r*-independent if any *r* of its elements  $X_{i_1}, \dots, X_{i_r}$  are statistically independent,*

$$\mathbb{P}[X_{i_1} = b_1, \dots, X_{i_r} = b_r] = \prod_{l=1}^r \mathbb{P}[X_{i_l} = b_l], \quad (11)$$

for any  $i_1 \neq \dots \neq i_r$  in the range  $[1, N]$  and  $b_i \in \{0, 1\}$ .

**Definition 2** (*r*-independent Pseudo-Wigner Ensemble of order  $N$ ). *Let a subset  $\mathcal{A}_N^r \subset S_N$  be endowed with the uniform measure. We say that it is an *r*-independent pseudo-Wigner Ensemble of order  $N$  if the elements of the upper triangular (including the main diagonal) parts of its matrices form an *r*-independent sequence w.r.t. (with respect to) the measure induced on them by  $\mathcal{A}_N^r$ .*

Below, whenever a probability over  $\mathcal{A}_N^r$  is considered, it is always implied to be w.r.t. to the uniform measure as in Definition 2. When the order  $r$  is clear from the context, we suppress it and write  $\mathcal{A}_N$ . Also denote by

$$\beta_{l,N} = \mathbb{E}[\beta_l(\mathbf{A}_N)] \quad (12)$$

the expected moments over an ensemble  $\mathcal{A}_N$ . The next result justifies the title ‘‘pseudo-Wigner’’ in the above definition.

**Lemma 2.** *Let  $\gamma \in \mathbb{N}$  and  $\mathbf{A}_N$  be chosen uniformly from  $\mathcal{A}_N^{2\gamma r}$  with  $r \geq l$ , then for the expected moments we have*

$$\beta_{l,N} = \begin{cases} 0, & l \text{ odd}, \\ \beta_l + o(1), & l \text{ even}, \end{cases} \quad (13)$$

as  $N \rightarrow \infty$ . In addition, the first  $p = 1, \dots, 2\gamma$  moments of the random variable  $N(\beta_l(\mathbf{A}_N) - \beta_{l,N})$  converge to the moments of the normal law,

$$M_p(N\beta_l(\mathbf{A}_N)) = \begin{cases} 0, & p \text{ odd}, \\ \frac{(p-1)!!}{\pi^{p/2}} + o(1), & p \text{ even}. \end{cases} \quad (14)$$

*Proof.* The proof follows that of the Main Theorem (Lemma 1 above) from [20] and is based on

counting paths of lengths up to  $2\gamma l$ . An essential ingredient of the proof consists in showing that the principal contribution to the even moments is made by simple even paths (paths in which every edge is passed exactly twice), therefore, the resulting moments only depend on the variances of the matrix entries and not on their higher moments (universality). Due to the  $2\gamma r$ -independence with  $r \geq l$ , the calculation of the expected values of products of matrix variables on such paths (see formula (4.3) from [20]) will give exactly the same results. This completes the proof.  $\square$

Our next goal is to control the deviations of the spectra of matrices  $\mathbf{A}_N \in \mathcal{A}_N$  from the semicircular law. For this purpose we use smoothing techniques based on finite polynomial expansions of the characteristic functions of the distributions at hand.

**Lemma 3** (Lemma 7.4.2 from [21]). *Suppose  $F$  is a c.d.f. and  $G : \mathbb{R} \rightarrow \mathbb{R}$  has bounded variation*

$$\int_{-\infty}^{+\infty} |G'(x)| dx < +\infty, \quad (15)$$

*bounded derivative*

$$M = \sup_x |G'(x)| < +\infty, \quad (16)$$

*and satisfies*

$$\lim_{x \rightarrow -\infty} G(x) = 0, \quad \lim_{x \rightarrow +\infty} G(x) = 1. \quad (17)$$

*Assume also that*

$$\int_{-\infty}^{\infty} |F(x) - G(x)| dx < \infty, \quad (18)$$

*and denote by  $\phi(t)$  and  $\gamma(t)$  the Fourier transforms of  $F(x)$  and  $G(x)$  correspondingly. then for any  $T > 0$ ,*

$$|F(x) - G(x)| \leq \frac{2}{\pi} \int_0^T \frac{|\phi(t) - \gamma(t)|}{t} dt + \frac{24M}{\pi T}, \quad (19)$$

*uniformly over  $x \in \mathbb{R}$ .*

**Theorem 1.** *Let  $q < e$ , then for<sup>1</sup>  $r \leq q \log_2 N$  and any  $\alpha \in (\frac{q}{e}, 1)$  there exists  $N_0$  such that for any  $N \geq N_0$ , with probability at least  $1 - \frac{\tau}{N^{2(1-\alpha)}}$ , a matrix  $\mathbf{A}_N$  chosen uniformly from  $\mathcal{A}_N^{2r}$  satisfies*

$$|F_{\mathbf{A}_N}(x) - F_{sc}(x)| \leq \frac{1}{r}, \quad \forall x \in \mathbb{R}. \quad (20)$$

<sup>1</sup>Here we imply that we may consider a sequence of pseudo-Wigner ensembles.

*Proof.* The proof is based on the application of Chebyshev's inequality and can be found in Appendix A.  $\square$

The same technique as in the proof of Theorem 1 applied to higher moments yields

**Theorem 2.** *Let  $\gamma \in \mathbb{N}$  and  $q < e$ , then for  $r \leq q \log_2 N$  and any  $\alpha \in (\frac{q}{e}, 1)$  there exists  $N_0$  such that for any  $N \geq N_0$ , with probability at least  $1 - \frac{3r(2\gamma-1)!!}{(\sqrt{\pi}N^{1-\alpha})^{2\gamma}}$ , a matrix  $\mathbf{A}_N$  chosen uniformly from  $\mathcal{A}_N^{2\gamma r}$  satisfies*

$$|F_{\mathbf{A}_N}(x) - F_{sc}(x)| \leq \frac{1}{r}, \quad \forall x \in \mathbb{R}. \quad (21)$$

*Proof.* The proof is based on the high-moments version of Chebyshev's inequality and can be found in Appendix A.  $\square$

#### IV. AN EXPLICIT CONSTRUCTION OF PSEUDO-WIGNER MATRICES FROM BCH CODES

We start from defining BCH codes and discussing the properties of their dual codes. Later we use these properties to explicitly construct an example of a pseudo-Wigner ensemble.

##### A. The BCH Code and its Dual Code

We focus specifically on BCH codes for the following reasons:

- the construction of BCH codes allows to control their minimum distances in an easy manner, and
- for relatively small designed minimum distances, the dimension of the obtained BCH codes are close to being maximal possible (consult section 1.10 from [22] for details).

For  $m \in \mathbb{N}$ , a primitive narrow-sense binary BCH code  $\mathcal{C}_m^\delta$  of length  $n = 2^m - 1$  and designed minimum distance  $\delta \geq 3$  is a cyclic linear code generated by the lowest degree binary polynomial having roots  $\alpha, \alpha^2, \dots, \alpha^{\delta-2}$ , where  $\alpha$  is a primitive element of  $GF(2^m)$ .

**Theorem 3** (Theorems 9.1.1, 9.9.18 and Corollary 9.3.8 from [22]). *A binary BCH code  $\mathcal{C}_m^\delta$  of length  $n = 2^m - 1$  and designed distance  $\delta = 2t + 1$  with  $2t - 1 < 2^{\lfloor m/2 \rfloor} + 1$*

- *has minimum distance  $d$  at least  $\delta$ ,*
- *has dimension  $2^m - 1 - mt$ .*

Note that the dimension  $2^m - 1 - mt$  is exactly characterized when the designed distance is small. Under the same assumptions as in Theorem 3, the dual BCH code has minimum distance at least  $d^\perp \geq d$ , dimension  $k^\perp = mt$  [22], and is also a cyclic code.

**Lemma 4** (Lemma 3.2 from [23]). *If a code  $\mathcal{C}$  has minimum distance  $d$ , then its dual code  $\mathcal{C}^\perp$  is  $(d-1)$ -independent w.r.t. to the uniform measure over its codewords.*

For  $N \in \mathbb{N}$ , let  $m \in \mathbb{N}$  be such that

$$2^{m-1} - 1 < \frac{N(N+1)}{2} \leq 2^m - 1. \quad (22)$$

Fix  $\delta$  small enough (Theorem 3) and construct a BCH code  $\mathcal{C}_m^\delta$ , whose parameters would be  $[2^m - 1, 2^m - 1 - \frac{(\delta-1)m}{2}, d]$  with  $d \geq \delta$ . For every word in the dual code  $\mathbf{c} = \{c_i\}_{i=1}^{2^m-1} \in (\mathcal{C}_m^\delta)^\perp$ , let  $\mathbf{b} = \zeta(\mathbf{c})$ . Construct a  $N \times N$  matrix  $\overline{\mathbf{B}}_N$  by filling its upper triangular part (including the main diagonal) with the first  $\frac{N(N+1)}{2}$  elements of the obtained sequence  $\mathbf{b}$  in any specific order (e.g. fill the upper triangular part row by row) and then reflect it w.r.t. to the main diagonal. Normalize the matrix  $\mathbf{B}_N = \frac{1}{2\sqrt{N}} \overline{\mathbf{B}}_N$ . The dimension of the dual code is  $\dim(\mathcal{C}_m^\delta)^\perp = \frac{(\delta-1)m}{2}$ . By Lemma 4, this construction gives us a set  $\mathcal{B}_N^{d-1}$  of matrices  $\mathbf{B}_N$ , which endowed with the uniform probability measure becomes a  $d-1$ -independent pseudo-Wigner ensemble of order  $N$  with  $d-1 \geq \delta-1$ . Since  $\mathcal{B}_N^{d-1}$  is also a  $\mathcal{B}_N^{\delta-1}$  ensemble and  $d$  may not be known, below we denote it by  $\mathcal{B}_N^{\delta-1}$  to simplify notations.

For example, for  $\delta = 2m + 1$  we obtain the following

**Theorem 4.** *There exists  $N_0$  such that for any  $N \geq N_0$ , if a matrix  $\mathbf{B}_N$  is chosen uniformly from  $\mathcal{B}_N^{[2\log_2 N]}$ , then with probability at least  $1 - \frac{2\log_2 N}{N^{6/5}}$ ,*

$$|F_{\mathbf{B}_N}(x) - F_{sc}(x)| \leq \frac{1}{\log_2 N}, \quad \forall x \in \mathbb{R}. \quad (23)$$

*Proof.* Follows directly from Theorem 1 by setting  $q = 1$  and  $\alpha = \frac{2}{5}$ .  $\square$

## V. THE KOLMOGOROV COMPLEXITY OF THE SEMICIRCULAR LAW

The standard computer scientific approach to quantify the amount of randomness contained in a piece of data  $\mathcal{D}$ , or its algorithmic compressibility, is based on calculating the length of a minimal

program creating that data on a universal Turing machine. The length of the obtained binary code is called the Kolmogorov complexity of the object and we denote it by  $\mathcal{KC}(\mathcal{D})$ . A comparison of Kolmogorov complexities of various objects of the same size is usually done by conditioning on that size  $\mathcal{KC}(\mathcal{D}|\text{size})$ , or in other words by assuming that it is already known to the machine [18].

The notion of Kolmogorov complexity is naturally defined for specific instances of data. Our goal is to generalize and extend this concept to classes of objects sharing a specific property or, in other words, to sets of objects. As an example, let us consider the following property

$$\mathcal{P}(N, \varepsilon) = \{\mathbf{A}_N \in S_N \mid \sup_x |F_{\mathbf{A}_N}(x) - F_{sc}(x)| \leq \varepsilon\}, \quad (24)$$

which is the set of symmetric  $\frac{1}{2\sqrt{N}}$ -scaled sign matrices of order  $N$  having spectra at most  $\varepsilon$  far from the semicircular law in Kolmogorov metric. A naturally arising question can be formulated as: What is the smallest Kolmogorov complexity of a matrix from this set? This is the length of the shortest binary program needed to construct an object of a specific size possessing the necessary property. We suggest to take this quantity as the measure of randomness, or complexity, of the property. Motivated by this intuition, we suggest the following formal definition

**Definition 3.** *The Kolmogorov complexity of a finite set (property)  $\mathcal{P}$  is defined as*

$$\mathcal{KC}(\mathcal{P}) = \min_{\mathcal{D} \in \mathcal{P}} \mathcal{KC}(\mathcal{D}). \quad (25)$$

The conditional Kolmogorov complexity is defined analogously.

Next we investigate the Kolmogorov complexity of the semicircular property. Given a binary polynomial  $f(x)$  of degree  $m$ , we write

$$\tilde{f}(x) = x^m f(x^{-1}) \quad (26)$$

for its reciprocal.

**Proposition 1.** *For  $\varepsilon \geq \frac{1}{\log_2 N}$ , the conditional Kolmogorov complexity of the property  $\mathcal{P}(N, \varepsilon)$  is bounded by*

$$\mathcal{KC}(\mathcal{P}(N, \varepsilon)|N) \leq \frac{2}{\varepsilon} \log_2 N + c, \quad (27)$$

where  $c$  does not depend on  $N$  or  $\varepsilon$ .

A matrix sampled uniformly from  $\mathcal{B}_N^{\lceil \frac{2}{\varepsilon} \rceil}$  provides an explicit construction with probability at least  $1 - \frac{1}{\varepsilon N^{6/5}}$ .

*Proof.* Theorem 1 guarantees that if the parameters of a pseudo-Wigner ensemble are chosen appropriately as functions of  $\varepsilon$ , at least one of the matrices from that ensemble must lie in the set  $\mathcal{P}(N, \varepsilon)$ . We will use this observation to obtain the desired bound on the Kolmogorov complexity of the property  $\mathcal{P}(N, \varepsilon)$ .

Our goal is, thus, to build a dual BCH code with the minimum designed distance of the original code  $\delta = \delta(\varepsilon)$ , construct a pseudo-Wigner ensemble of  $N \times N$  matrices based on it, and specify one matrix from there. Table Algorithm 1 contains *pseudo-code* implementing the described algorithm. Note that the constructed matrix belongs to a  $\delta - 1$  independent pseudo-Wigner ensemble and Theorem 1, therefore, bounds the discrepancy of the c.d.f.s.

The upper bound on the Kolmogorov complexity is obtained by bounding the length of the algorithm's description. Note that the description of the Initialization step in Algorithm 1 requires at most

$$\log_2 2^m + \log_2 2^{\frac{(\delta-1)m}{2}} + c_1 = m + \frac{(\delta-1)m}{2} + c_1 \quad (28)$$

bits to define polynomials  $f(x)$  and  $v(x)$  (represented by binary coefficient vectors  $\mathbf{f}$  and  $\mathbf{v}$ ) [18]. At this stage the algorithm copies the values of  $\mathbf{f}$  and  $\mathbf{v}$  into the memory and the remaining code accesses them by their addresses, therefore, the description of steps 1–11 have constant complexity not depending on  $m$  or  $\delta$ . Overall, we get the following upper bound on the Kolmogorov complexity

$$\mathcal{L} \leq \frac{(\delta+1)m}{2} + c, \quad (29)$$

where  $c$  does not depend on  $m$  or  $\delta$ . Theorem 1 implies that the relation between the precision and the designed minimum distance is  $\delta \sim \frac{2}{\varepsilon}$ , which together with (22) yields (27).

Now set  $r = \lceil \frac{1}{\varepsilon} \rceil$  and invoke Theorem 1 with  $\alpha = \frac{2}{5}$  to construct the necessary pseudo-Wigner ensemble and obtain the desired statement.  $\square$

Proposition 1 demonstrates that the Kolmogorov complexity of property  $\mathcal{P}(N, \varepsilon)$  for moderate values of  $\varepsilon$  is proportional to  $\frac{1}{\varepsilon} \log_2 N$  and is relatively small.

---

### Algorithm 1: Pseudo-Wigner Matrix

---

**Input:**  $\mathbf{f} \in GF(2)^m, \mathbf{v} \in GF(2)^{\frac{(\delta-1)m}{2}}$

**Output:**  $\mathbf{B}_N$ , s.t.  $|F_{\mathbf{B}_N}(x) - F_{sc}(x)| \leq \frac{2}{\delta-1}$ .

*Initialization :* read  $\mathbf{f}, \mathbf{v}$  and  $\delta$  into memory;

- 1: construct  $f(x) = \sum_j f_j x^j, v(x) = \sum_j v_j x^j$ ,
  - 2: build a splitting field  $\mathcal{F}$  of  $x^{2^m-1} - 1$ , which is also a splitting field for  $f(x)$ ;
  - 3: let  $\alpha \in \mathcal{F}$  be any root of  $f(x)$ ,  $f(\alpha) = 0$ ;
  - 4: **for**  $j = 2: \delta - 2$  **do**
  - 5:   find the min. polynomial  $f_j(x)$  of  $\alpha^j \in \mathcal{F}$ ;
  - 6:   **if**  $f_j(x) \nmid f(x)$  **then**
  - 7:      $f(x) \leftarrow f(x)f_j(x)$ ;
  - 8:   **end if**
  - 9: **end for**
  - 10:  $h(x) \leftarrow \frac{x^{2^m-1} - 1}{\tilde{f}(x)}$ ;
  - 11: take the codeword  $\mathbf{c}$ , whose polynomial representation is  $v(x)h(x)$  and build  $\mathbf{B}_N$  as described in Section IV-A;
- 

## VI. QUASI-RANDOM GRAPHS

In this section we compare the proposed pseudo-Wigner matrices with the adjacency matrices of quasi-random Graphs from [19]. Given a symmetric binary adjacency  $\mathbf{T}_N = \{t_{ij}\}$  matrix of an undirected graph on  $N$  vertices, we apply to it  $\zeta$  transformation from (2) to get a sign matrix  $\mathbf{Q}_N = \{q_{ij}\}$  (in (2)  $\zeta$  was defined on sequences, however, a generalization to matrices is straightforward). The relation between  $\mathbf{T}_N$  and  $\mathbf{Q}_N$  can be written as

$$\mathbf{T}_N = \frac{1}{2} (\mathbf{1} \cdot \mathbf{1}^T + \mathbf{Q}_N), \quad (30)$$

where  $\mathbf{1} = [1, \dots, 1]^T$  is a column vector of height  $N$ . As shown in [19], if a graph<sup>2</sup> satisfies condition  $P_3$  given on page 347, it is a quasi-random graph. This condition can be formulated in terms of the adjacency matrix  $\mathbf{T}_N$  as following. Let  $N \rightarrow +\infty$ , then if

- 1) the number of non-zero elements in  $\mathbf{T}_N$  is  $\sum_{ij} t_{ij} = \frac{N^2}{2} + o(N^2)$  (we have 2 in the denominator instead of 4 because we count all the edges twice due to the symmetry of the adjacency matrix),

<sup>2</sup>To be precise, we should talk about sequences of graphs and their corresponding adjacency matrices. However, following [19] to simplify the notations of this section and to better convey the intuition behind the calculations we prefer to talk about single instances of graphs and matrices.

- 2)  $\lambda_1(\mathbf{T}_N) = \frac{N}{2} + o(N)$ ,  
 3)  $\lambda_2(\mathbf{T}_N) = o(N)$ ,

then the underlying graph is quasi-random.

To demonstrate that our pseudo-Random matrices may serve as a source of quasi-random graphs with high probability, let us show the following

**Lemma 5.** *For a matrix  $\mathbf{A}_N \in \mathcal{A}_N^d$  and any vector  $\mathbf{x} \in \mathbb{R}^N$ ,  $\|\mathbf{x}\| = 1$ ,*

$$\mathbb{P}[\mathbf{x}^T \mathbf{A}_N \mathbf{x} \geq 1] \leq \frac{1}{N}. \quad (31)$$

*Proof.* The proof can be found in Appendix B.  $\square$

Recall that the spectral norm of a symmetric real matrix is defined as

$$\|\mathbf{Q}_N\| = \max_{\mathbf{x}, \|\mathbf{x}\|=1} \mathbf{x}^T \mathbf{Q}_N \mathbf{x}, \quad (32)$$

and note that we need to multiply matrix  $\mathbf{A}_N$  by  $2\sqrt{N}$  to get a sign matrix  $\mathbf{Q}_N = 2\sqrt{N}\mathbf{A}_N$ . Now as a corollary of Lemma 5, we get

$$\mathbb{P}[\|\mathbf{Q}_N\| \geq 2\sqrt{N}] \leq \frac{1}{N}, \quad (33)$$

and, therefore, with high probability  $\|\mathbf{Q}_N\| = o(N)$ .

**Lemma 6** (Weyl's Theorem, [24]). *Let the eigenvalues of real symmetric  $N \times N$  matrices  $\mathbf{L}$  and  $\mathbf{L} + \mathbf{N}$  be  $\lambda_1 \geq \dots \geq \lambda_N$  and  $\nu_1 \geq \dots \geq \nu_N$  correspondingly, then*

$$\max_i \|\lambda_i - \nu_i\| \leq \|\mathbf{N}\|. \quad (34)$$

Note that relation (30) may be viewed as a perturbation of matrix  $\frac{1}{2}\mathbf{1} \cdot \mathbf{1}^T$ , whose eigenvalues are  $\lambda_1 = \frac{N}{2}$  and  $\lambda_2 = \dots = \lambda_{N-1} = 0$ . Weyl's theorem together with (33) immediately implies that with high probability,

$$\lambda_1(\mathbf{T}_N) = \frac{N}{2} + o(N), \quad \lambda_2(\mathbf{T}_N) = o(N). \quad (35)$$

In addition, set  $\mathbf{x} = \frac{1}{\sqrt{N}}\mathbf{1}$  to get

$$\mathbb{P}\left[\sum_{ij} q_{ij} \geq 2N^{3/2}\right] \leq \frac{1}{N}, \quad (36)$$

which implies that  $\sum_{ij} q_{ij} = o(N^2)$ , or

$$\sum_{ij} t_{ij} = \frac{N^2}{2} + o(N^2), \quad (37)$$

as required. Therefore, we see that matrices from a pseudo-Wigner ensemble  $\mathcal{A}_N^2$  with high probability exhibit properties of quasi-random graphs.

This simple example sheds more light on the hierarchy of properties of random graphs/matrices. We can conclude that if we have a sequence of pseudo-Wigner matrices of growing dimensions with fixed independence order  $d(N) = d$ , then we are more or less in the case of quasi-random graphs. Quasi-random graphs can be hardly considered random, as Paley graphs example demonstrates [19]. A higher level of complexity is the semicircular law, where we require  $d(N)$  to grow with the size of the matrices. It can be in fact easily shown that the rate of growth of  $d(N)$  only affects the speed of convergence, but not the limiting spectral law.

## VII. NUMERICAL SIMULATIONS

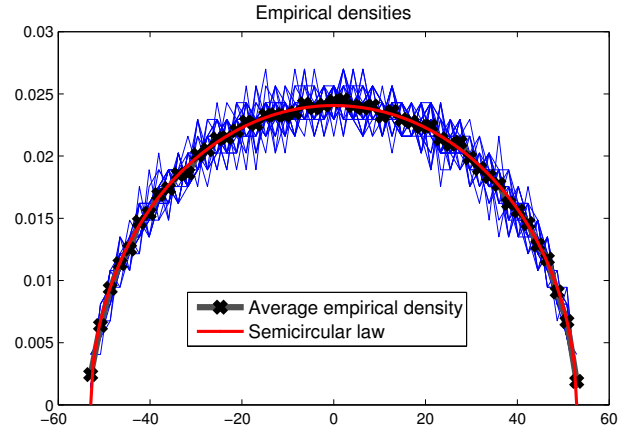


Fig. 1: Empirical spectral densities of 25 pseudo-Wigner matrices,  $N = 700$ ,  $m = 18$ .

To demonstrate the power of the above construction, we chose  $m = 18$ ,  $N = 700$  and constructed an ensemble  $\mathcal{B}_N^2$ . In this case  $d = 3$  and the code  $\mathcal{C}$  may be built by choosing a primitive polynomial of order  $m$  and using it as a linear feedback shift register to generate a Golomb sequences [5], which is then cyclically shifted to get the entire code. In our simulation we picked  $f(x) = x^{18} + x^7 + 1$ . Figure 1 shows the empirical spectra of 25 matrices  $\mathbf{B}_N \in \mathcal{B}_N^2$ , their average spectrum and compare them to the semicircular law.

## VIII. CONCLUSIONS

In this article we consider the problem of defining and generating ensembles of pseudo-random matrices based on the similarity of their spectra to the semicircular density. We introduce  $r$ -independent pseudo-Wigner ensembles and prove

their closeness to the semicircular law. We give an explicit construction of such ensembles using the dual BCH codes and compare them to the quasi-random graphs proposed by Chung, Graham and Wilson. We demonstrate that the Kolmogorov complexity of the proposed construction is proportional to  $\frac{1}{\varepsilon} \log_2 N$ , where  $\varepsilon$  is a precision parameter, which is comparatively small. Finally, we justify the proposed construction numerically.

## APPENDIX A

*Proof of Theorem 1.* The probability measures defined by the c.d.f.-s  $F_{sc}(x)$  and  $F_{\mathbf{A}_N}(x)$  are compact, therefore,

$$\int_{-\infty}^{\infty} |F_{\mathbf{A}_N}(x) - F_{sc}(x)| dx < \infty. \quad (38)$$

The derivative of  $F_{sc}$  is the semicircular p.d.f.  $f_{sc}$  given in (6), and is bounded by

$$M = \sup_x |f_{sc}(x)| = f_{sc}(0) = \frac{2}{\pi}. \quad (39)$$

Recall also that the total variation of a differentiable c.d.f. is always one and apply Lemma 3 to  $F_{\mathbf{A}_N}(x)$  (in place of  $F$ ) and  $F_{sc}(x)$  (in place of  $G$ ) to obtain

$$\begin{aligned} |F_{\mathbf{A}_N}(x) - F_{sc}(x)| \\ \leq \frac{2}{\pi} \int_0^T \frac{|\phi_{\mathbf{A}_N}(t) - \phi_{sc}(t)|}{t} dt + \frac{24M}{\pi T}. \end{aligned} \quad (40)$$

The  $\rho - 1$ -th order Mclaurin polynomial expansion of the exponential function with a remainder gives the bound (see Section XV.4, pages 512-514 from [25])

$$\left| e^{ixt} - 1 - \sum_{l=1}^{\rho-1} \frac{(it)^l}{l!} x^l \right| \leq \frac{t^\rho}{\rho!} |x|^\rho, \quad x, t \in \mathbb{R}, \quad t \geq 0. \quad (41)$$

For even  $\rho$ , after taking expectations for fixed  $t$  we get

$$\left| \phi_{sc}(t) - 1 - \sum_{l=1}^{\rho-1} \beta_l \frac{(it)^l}{l!} \right| \leq \beta_\rho \frac{t^\rho}{\rho!}. \quad (42)$$

Similarly,

$$\left| \phi_{\mathbf{A}_N}(t) - 1 - \sum_{l=1}^{\rho-1} \beta_l(\mathbf{A}_N) \frac{(it)^l}{l!} \right| \leq \beta_l(\mathbf{A}_N) \frac{t^\rho}{\rho!}. \quad (43)$$

Set

$$\rho = \begin{cases} r, & r \text{ even,} \\ 2\lfloor \frac{r-1}{2} \rfloor, & r \text{ odd.} \end{cases} \quad (44)$$

Use (42) and (43) to obtain the following bound on the integral summand of the right-hand side of (40),

$$\begin{aligned} \int_0^T \left| \frac{\phi_{\mathbf{A}_N}(t) - \phi_{sc}(t)}{t} \right| dt \\ \leq \int_0^T \frac{1}{t} \left| \sum_{l=1}^{\rho-1} \beta_l(\mathbf{A}_N) \frac{(it)^l}{l!} - \sum_{l=1}^{\rho-1} \beta_l \frac{(it)^l}{l!} \right| dt \\ + \int_0^T [\beta_\rho(\mathbf{A}_N) + \beta_\rho] \frac{t^{\rho-1}}{\rho!} dt \\ \leq \int_0^T \frac{1}{t} \left| \sum_{l=1}^{\rho-1} [\beta_l(\mathbf{A}_N) - \beta_l] \frac{(it)^l}{l!} \right| dt \\ + [\beta_\rho(\mathbf{A}_N) + \beta_\rho] \frac{T^\rho}{\rho \cdot \rho!} = S_1 + S_2. \end{aligned} \quad (45)$$

Bound  $S_1$  as

$$\begin{aligned} S_1 = \int_0^T \frac{1}{t} \left| \sum_{l=1}^{\rho-1} [\beta_l(\mathbf{A}_N) - \beta_l] \frac{(it)^l}{l!} \right| dt \\ \leq \max_{l=1}^{\rho-1} |\beta_l(\mathbf{A}_N) - \beta_l| \int_0^T \sum_{l=1}^{\rho-1} \frac{t^{l-1}}{l!} dt. \end{aligned} \quad (46)$$

From the triangle inequality,

$$|\beta_l(\mathbf{A}_N) - \beta_l| \leq |\beta_{l,N} - \beta_l| + |\beta_l(\mathbf{A}_N) - \beta_{l,N}|. \quad (47)$$

For the first summand we have

$$|\beta_{l,N} - \beta_l| \leq \frac{2\rho}{N}, \quad (48)$$

which follows directly from the path counting, see [26] for details.

By Lemma 2, the variance of the second summand of (47) satisfies

$$\text{var} [\beta_l(\mathbf{A}_N) - \beta_{l,N}] = \frac{1}{\pi N^2} + o\left(\frac{1}{N^2}\right), \quad N \rightarrow +\infty. \quad (49)$$

Therefore, there exists  $N_0 \in \mathbb{N}$  such that

$$\text{var} [\beta_l(\mathbf{A}_N) - \beta_{l,N}] \leq \frac{2}{\pi N^2}, \quad \forall N \geq N_0. \quad (50)$$

Now the Chebyshev bound gives starting from  $N_0$ ,

$$\mathbb{P} [|\beta_l(\mathbf{A}_N) - \beta_{l,N}| \geq \delta] \leq \frac{2}{\pi N^2 \delta^2}. \quad (51)$$

Apply the union bound to the maximum in (46) to get

$$\begin{aligned} \mathbb{P} \left[ \max_{l=1}^{\rho-1} |\beta_l(\mathbf{A}_N) - \beta_l| \geq \delta \right] &\leq \sum_{l=1}^{\rho-1} \mathbb{P} [|\beta_l(\mathbf{A}_N) - \beta_l| \geq \delta] \\ &\leq \frac{2(\rho-1)}{\pi N^2 \delta^2}. \end{aligned} \quad (52)$$



Note that for any  $a, b \in \mathbb{N}$ ,

$$\sum_{l=a}^b \frac{t^l}{l \cdot l!} \leq \sum_{l=0}^{+\infty} \frac{t^l}{l!} = e^t. \quad (53)$$

We conclude that

$$\int_0^T \sum_{l=1}^{\rho-1} \frac{t^{l-1}}{l!} dt \leq \sum_{l=1}^{\rho-1} \frac{T^l}{l \cdot l!} \leq e^T. \quad (54)$$

Overall, for  $S_1$  we have

$$\mathbb{P}\left[S_1 \geq \left(\delta + \frac{2\rho}{N}\right)e^T\right] \leq \frac{2(\rho-1)}{\pi N^2 \delta^2}. \quad (55)$$

Choose

$$\delta = \frac{1}{N^\alpha}, \quad (56)$$

and let

$$T = \frac{\rho^{1+1/\rho}}{e}. \quad (57)$$

Recall the assumptions:  $\alpha < 1$  and

$$\rho \leq q \log_2 N, \quad (58)$$

to get for  $N \geq N_0$  large enough,

$$\begin{aligned} \left(\delta + \frac{2\rho}{N}\right)e^T &\leq \left(\frac{1}{N^\alpha} + \frac{2q \log_2 N}{N}\right)e^{\rho/e} e^{\varrho/\bar{\rho}} \\ &\leq \frac{1}{N^\alpha} N^{\frac{q}{e}} e^{\varrho/\bar{\rho}}, \end{aligned} \quad (59)$$

and, therefore,

$$\mathbb{P}\left[S_1 \geq \frac{e^{\varrho/\bar{\rho}}}{N^{\alpha-\frac{q}{e}}}\right] \leq \frac{2(\rho-1)}{\pi N^{2(1-\alpha)}}. \quad (60)$$

Using the same Chebyshev bound (51) and the triangle inequality, for the second summand on the right-hand side of (45) we obtain

$$\mathbb{P}\left[S_2 \geq \left(2\beta_\rho + \eta + \frac{2\rho}{N}\right) \frac{T^r}{\pi \rho \cdot \rho!}\right] \leq \frac{2}{\pi N^2 \eta^2}. \quad (61)$$

Use Stirling's approximation

$$\sqrt{2\pi} \rho^{\rho+\frac{1}{2}} e^{-\rho} \leq \rho! \leq e \rho^{\rho+\frac{1}{2}} e^{-\rho}, \quad (62)$$

to get from (7) the following bound

$$\beta_\rho = \frac{1}{2^\rho} \frac{\rho!}{\left(\frac{\rho}{2}\right)! \left(\frac{\rho}{2} + 1\right)!} \leq \frac{2}{\rho^{3/2}}. \quad (63)$$

Plug this result into (61), recall (58), and set  $\eta = \frac{1}{\rho^{3/2}}$  to get

$$\mathbb{P}\left[S_2 \geq \frac{1}{\rho^{5/2}} \frac{T^\rho}{\rho!}\right] \leq \frac{2\rho^3}{\pi N^2}. \quad (64)$$

Now use (57) to obtain

$$\frac{1}{\rho^{5/2}} \frac{T^\rho}{\rho!} \leq \frac{1}{\rho^2}, \quad (65)$$

and, thus,

$$\mathbb{P}\left[S_2 \geq \frac{1}{\rho^2}\right] \leq \frac{2\rho^3}{\pi N^2}. \quad (66)$$

Finally, using the inequality (58) again, we get from (60) and (66) that for  $N \geq N_0$  large enough,

$$\begin{aligned} \mathbb{P}\left[S_1 + S_2 \geq \frac{2}{\rho^2}\right] &\leq \frac{2\rho^3}{\pi N^2} + \frac{2\rho}{\pi N^{2(1-\alpha)}} \\ &\leq \frac{3\rho}{\pi N^{2(1-\alpha)}} \leq \frac{\rho}{N^{2(1-\alpha)}}, \end{aligned} \quad (67)$$

where we have used the union bound and noted that in order for the sum  $S_1 + S_2$  to be greater than  $\frac{2}{\rho^2}$ , at least one of the summands must necessarily be greater than  $\frac{1}{\rho^2}$ . Altogether, with probability at least  $1 - \frac{\rho}{N^{2(1-\alpha)}}$ ,

$$\int_0^T \frac{1}{t} \left| \sum_{l=1}^{\rho-1} [\beta_l(\mathbf{A}_N) - \beta_l] \frac{(it)^l}{l!} \right| dt \leq \frac{2}{\rho^2}. \quad (68)$$

Plug this bound and (57) into (40) to conclude that with probability at least  $1 - \frac{\rho}{N^{2(1-\alpha)}}$ ,

$$|F_{\mathbf{A}_N}(x) - F_{sc}(x)| \leq \frac{2}{\rho^2} + \frac{24eM}{\rho^{1+1/\rho}}. \quad (69)$$

From (6) we have

$$M = \frac{2}{\pi}, \quad (70)$$

therefore, for  $N \geq N_0$  large enough,

$$|F_{\mathbf{A}_N}(x) - F_{sc}(x)| \leq \frac{1}{\rho}. \quad (71)$$

Recall (44) to conclude the proof.  $\square$

**Remark 1.** Note that unlike [23], we cannot apply Lemma XVI.3.2 from [25] to prove Theorem 1, since in our case the empirical spectral measures  $F_{\mathbf{A}_N}(x)$  are in general not centered. Due to this distinction, we use another smoothing inequality given by Lemma 3.

*Proof of Theorem 2.* The proof goes along the lines of the proof of Theorem 1 up to equation (51), where we use a stronger version of Chebyshev inequality for higher moments, namely,

$$\mathbb{P}[|X - \mathbb{E}X| \geq \delta] \leq \frac{M_p(X)}{\delta^p}, \quad (72)$$

where  $X$  is a random variable with a finite  $p$ -th absolute moment

$$\overline{M}_p(X) = \mathbb{E}[|X - \mathbb{E}X|^p]. \quad (73)$$

Since according to Lemma 2

$$N(\beta_l(\mathbf{A}_N) - \beta_{l,N}) \xrightarrow{D} \mathcal{N}\left(0, \frac{1}{\pi}\right), \quad (74)$$

for  $l \leq \rho$  with  $\rho$  as in (44), the absolute moments read as

$$\mathbb{E}[|\beta_l(\mathbf{A}_N) - \beta_{l,N}|^p] = \frac{(p-1)!!}{(\sqrt{\pi}N)^p} \cdot \begin{cases} \sqrt{\frac{2}{\pi}}, & p \text{ even,} \\ 1, & p \text{ odd} \end{cases} + o\left(\frac{1}{N^p}\right), \quad n \rightarrow +\infty. \quad (75)$$

Therefore, there exists  $N_0$  such that

$$M_p(\beta_l(\mathbf{A}_N)) \leq \frac{2(p-1)!!}{(\sqrt{\pi}N)^p}, \quad \forall N \geq N_0. \quad (76)$$

Now Chebyshev bound (72) implies that starting from  $N_0$ ,

$$\mathbb{P}[|\beta_l(\mathbf{A}_N) - \beta_l| \geq \delta] \leq \frac{2(p-1)!!}{(\sqrt{\pi}N\delta)^p}. \quad (77)$$

In our case we know that moments up to order  $2\gamma$  must coincide with those of the Wigner ensemble, therefore, we get

$$\begin{aligned} \mathbb{P}\left[\max_{l=1}^{\rho-1} |\beta_l(\mathbf{A}_N) - \beta_l| \geq \delta\right] &\leq \sum_{l=1}^{\rho-1} \mathbb{P}[|\beta_l(\mathbf{A}_N) - \beta_l| \geq \delta] \\ &\leq \frac{2(\rho-1)(2\gamma-1)!!}{(\sqrt{\pi}N\delta)^{2\gamma}}. \end{aligned} \quad (78)$$

Following the proof of Theorem 1 and using the bound in (77) instead of (51) we get the desired result.  $\square$

## APPENDIX B

*Proof of Lemma 5.* Introduce a random variable,

$$\xi = \mathbf{x}^T \mathbf{A}_N \mathbf{x}, \quad (79)$$

then  $\mathbb{E}[\xi] = 0$  and its variance reads as

$$\text{var}[\xi] = \mathbb{E}[(\mathbf{x}^T \mathbf{A}_N \mathbf{x})^2] = \mathbb{E}\left[\sum_{ijkl} x_i x_j x_k x_l a_{ij} a_{kl}\right],$$

where  $\mathbf{A}_N = \{a_{ij}\}_{i,j=1}^N$ . Since the elements from the upper triangular part of  $\mathbf{A}_N$  are pairwise independent, the only contribution to this expectation is

made by summands with  $i = k, j = l$  and  $i = l, j = k$ . Recall also that  $\mathbb{E}[a_{ij}^2] = \frac{1}{4N}$ , to get

$$\begin{aligned} \text{var}[\xi] &= 2\mathbb{E}\left[\sum_{ij} x_i^2 x_j^2 a_{ij}^2\right] = \frac{2}{4N} \sum_{ij} x_i^2 x_j^2 \\ &= \frac{1}{2N} \left(\sum_i x_i^2\right) \left(\sum_j x_j^2\right) = \frac{1}{2N}. \end{aligned} \quad (80)$$

Chebyshev's bound now yields

$$\mathbb{P}[\mathbf{x}^T \mathbf{A}_N \mathbf{x} \geq \delta] \leq \frac{1}{2N\delta^2}, \quad (81)$$

and by setting  $\delta = 1$  we obtain the desired statement.  $\square$

## REFERENCES

- [1] G. Akemann, J. Baik, and P. Di Francesco, "The Oxford handbook of random matrix theory," *Oxford University Press*, 2011.
- [2] E. P. Wigner, "Characteristic vectors of bordered matrices with infinite dimensions," *Annals of Mathematics*, vol. 62, no. 3, pp. 548–564, 1955.
- [3] J. E. Gentle, "Random number generation and Monte Carlo methods," *Springer Science & Business Media*, 2013.
- [4] H.-J. Zepernick and A. Finger, "Pseudo random signal processing: theory and application," *John Wiley & Sons*, 2013.
- [5] S. W. Golomb *et al.*, "Shift register sequences," *Aegean Park Press*, 1982.
- [6] I. Reed and R. Stewart, "Note on the existence of perfect maps," *IRE Transactions on Information Theory*, vol. 8, no. 1, pp. 10–12, 1962.
- [7] F. J. MacWilliams and N. J. A. Sloane, "Pseudo-random sequences and arrays," *Proceedings of the IEEE*, vol. 64, no. 12, pp. 1715–1729, 1976.
- [8] H. Imai, "A theory of two-dimensional cyclic codes," *Information and Control*, vol. 34, no. 1, pp. 1–21, 1977.
- [9] S. Sakata, "On determining the independent point set for doubly periodic arrays and encoding two-dimensional cyclic codes and their duals," *IEEE Transactions on Information Theory*, vol. 27, no. 5, pp. 556–565, 1981.
- [10] K. G. Paterson, "Perfect maps," *IEEE Transactions on Information Theory*, vol. 40, no. 3, pp. 743–753, 1994.

- [11] T. Etzion, “Constructions for perfect maps and pseudorandom arrays,” *IEEE Transactions on Information Theory*, vol. 34, no. 5, pp. 1308–1316, 1988.
- [12] P. Grunwald and P. Vitányi, “Shannon information and Kolmogorov complexity,” *arXiv preprint cs/0410002*, 2004.
- [13] M. Li and P. Vitányi, “An introduction to Kolmogorov complexity and its applications,” *Springer Science & Business Media*, 2009.
- [14] R. G. Downey and D. R. Hirschfeldt, “Algorithmic randomness and complexity,” *Springer Science & Business Media*, 2010.
- [15] R. J. Solomonoff, “A formal theory of inductive inference. Part I,” *Information and Control*, vol. 7, no. 1, pp. 1–22, 1964.
- [16] A. N. Kolmogorov, “Three approaches to the quantitative definition of information,” *Problems of Information Transmission*, vol. 1, no. 1, pp. 1–7, 1965.
- [17] D. E. Knuth, “The art of computer programming: seminumerical algorithms, vol. 2,” *Pearson Education*, vol. 3, 1998.
- [18] T. M. Cover and J. A. Thomas, “Elements of information theory,” *John Wiley & Sons*, 2012.
- [19] F. R. K. Chung, R. L. Graham, and R. M. Wilson, “Quasi-random graphs,” *Combinatorica*, vol. 9, no. 4, pp. 345–362, 1989.
- [20] Y. Sinai and A. Soshnikov, “Central limit theorem for traces of large random symmetric matrices with independent matrix elements,” *Boletim da Sociedade Brasileira de Matemática*, vol. 29, no. 1, pp. 1–24, 1998.
- [21] K. L. Chung, “A course in probability theory,” *Academic press*, 2001.
- [22] F. J. MacWilliams and N. J. A. Sloane, “The theory of error correcting codes,” *Elsevier*, 1977.
- [23] B. Babadi and V. Tarokh, “Spectral distribution of random matrices from binary linear block codes,” *IEEE Transactions of Information Theory*, vol. 57, no. 6, pp. 3955–3962, 2011.
- [24] H. Weyl, “Das asymptotische verteilungsgesetz der eigenwerte linearer partieller differentialgleichungen (mit einer anwendung auf die theorie der hohlraumstrahlung),” *Mathematische Annalen*, vol. 71, no. 4, pp. 441–479, 1912.
- [25] W. Feller, “Introduction to probability theory and its applications,” *John Wiley & Sons*, vol. II, 1966.
- [26] Z. Bai and J. W. Silverstein, “Spectral analysis of large dimensional random matrices,” *Springer*, vol. 20, 2010.